Fig.1

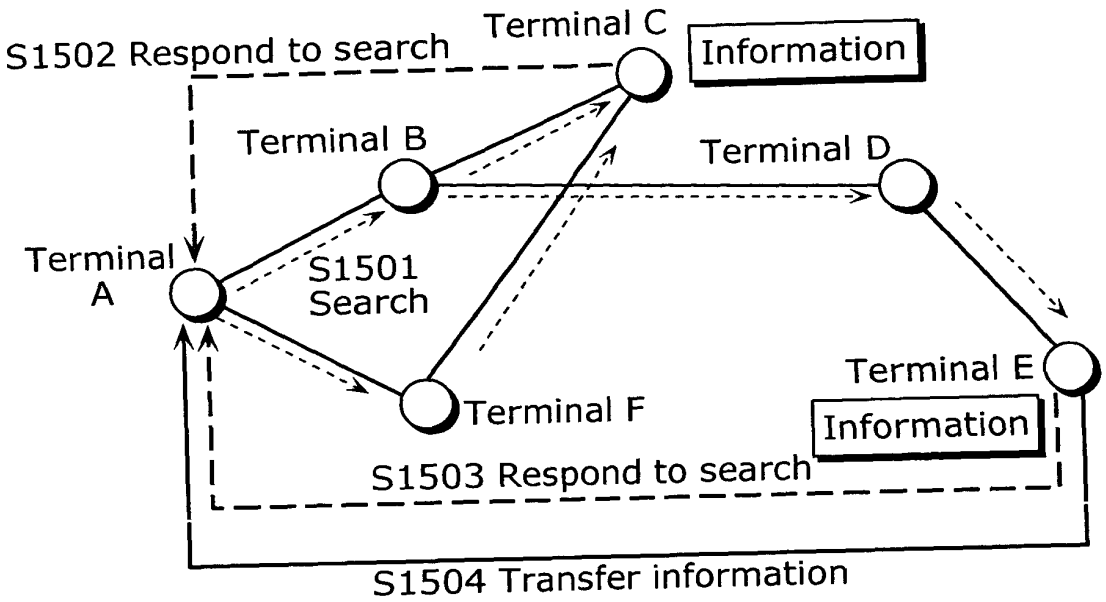

Terminal C
Information
S1502 Respond to search
Terminal B
Terminal D
Terminal A
S1501
Search
Terminal E
Information
Terminal F
S1503 Respond to search
S1504 Transfer information

Fig.2

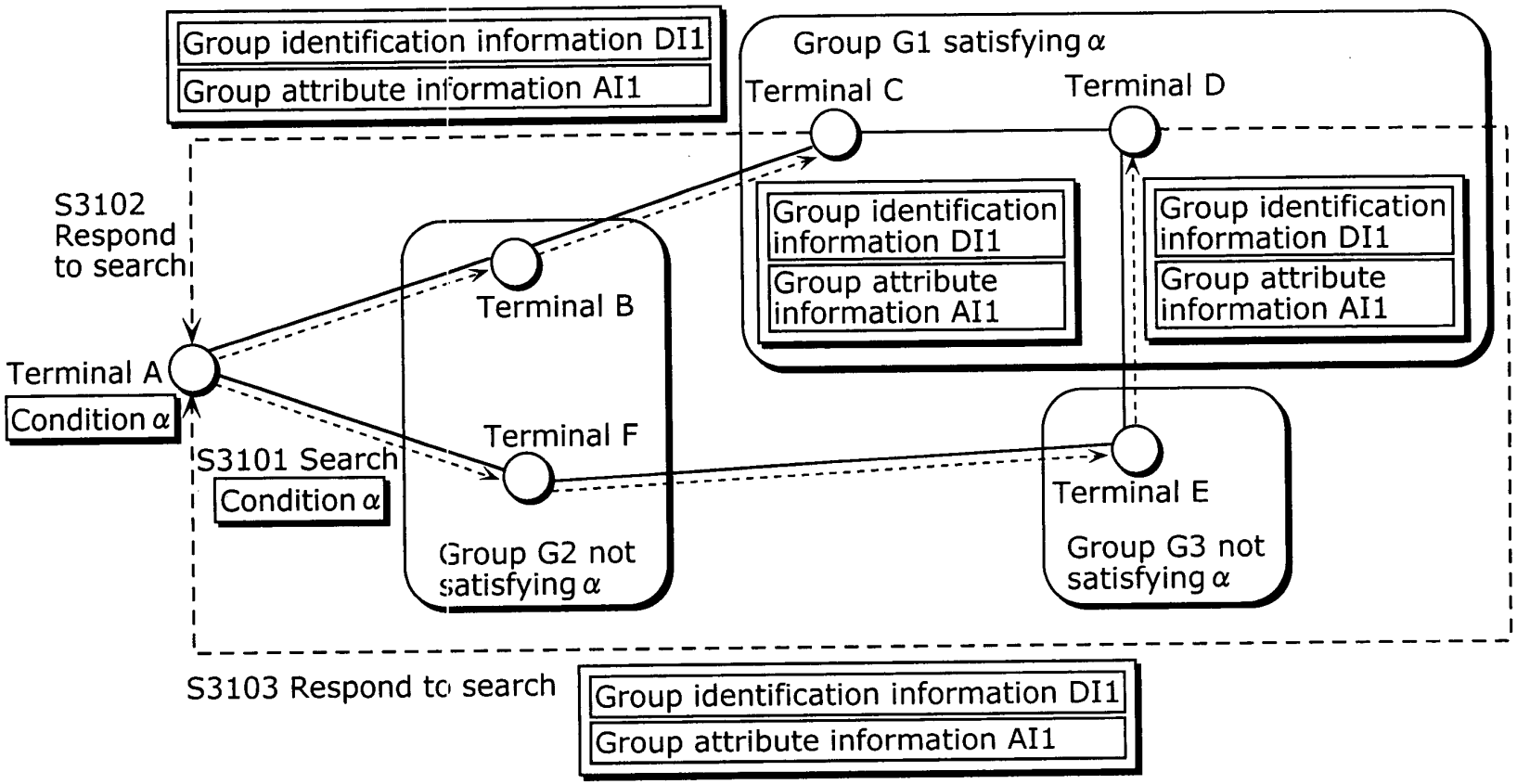

Group identification information DI1
Group attribute information AI1
Group G1 satisfying α
Terminal C
Terminal D
S3102
Respond
to search
Group identification information DI1
Group attribute information AI1
Group identification information DI1
Group attribute information AI1
Terminal B
Terminal A
Condition α
Terminal F
S3101 Search
Condition α
Terminal E
Group G2 not satisfying α
Group G3 not satisfying α
S3103 Respond to search
Group identification information DI1
Group attribute information AI1

Fig.3

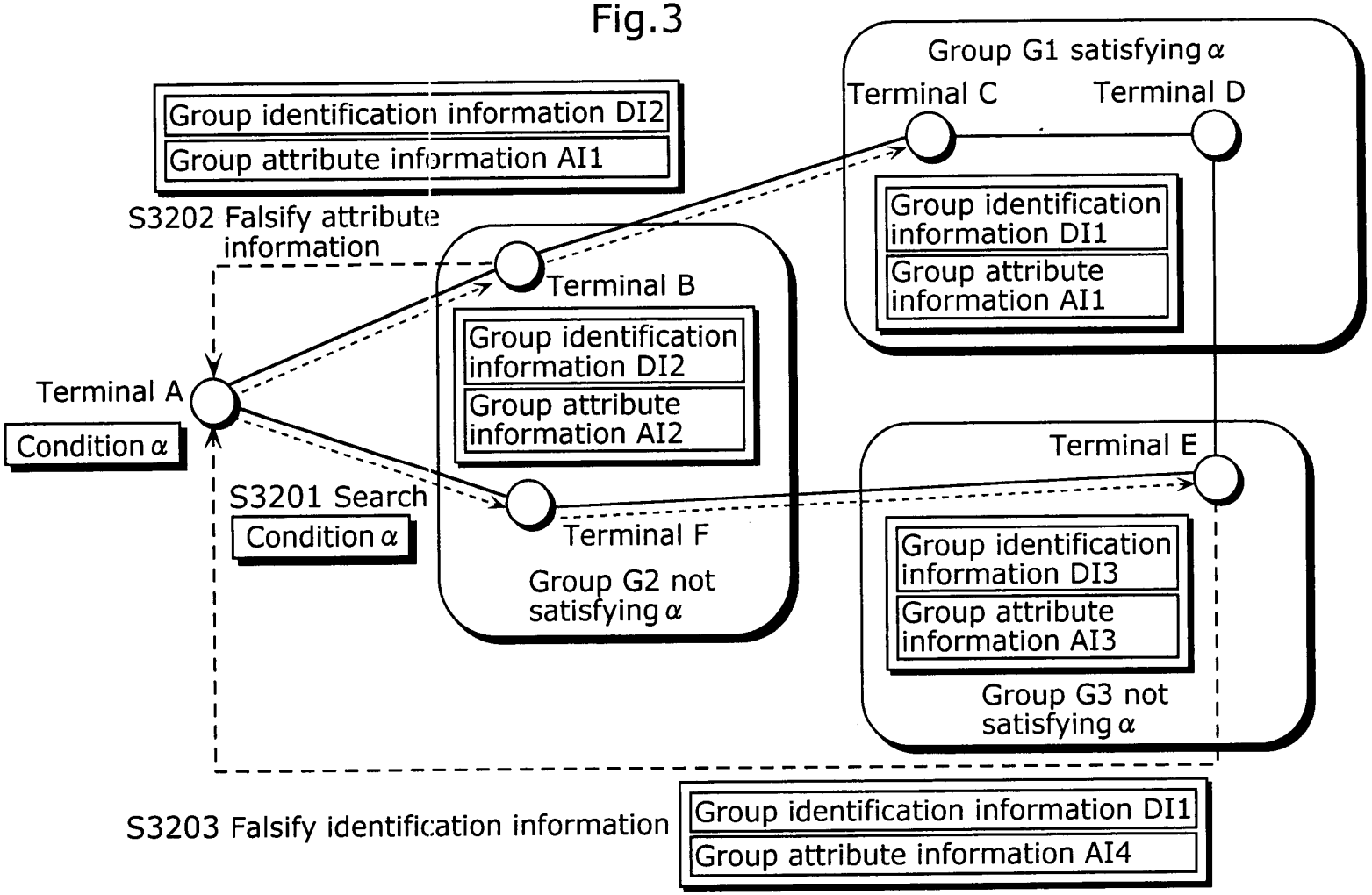

Group G1 satisfying α
Terminal C
Terminal D
Group identification information DI2
Group attribute information AI1
S3202 Falsify attribute information
Group identification information DI1
Group attribute information AI1
Terminal B
Group identification information DI2
Group attribute information AI2
Terminal A
Condition α
Terminal E
S3201 Search
Condition α
Terminal F
Group identification information DI3
Group attribute information AI3
Group G2 not satisfying α
Group G3 not satisfying α
S3203 Falsify identification information
Group identification information DI1
Group attribute information AI4

Fig.4A

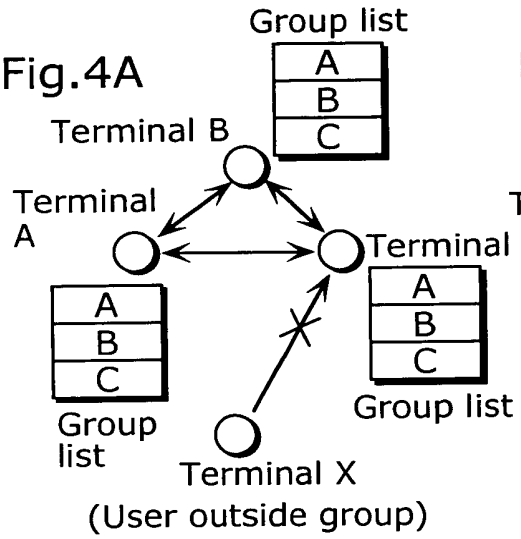


Fig.4B

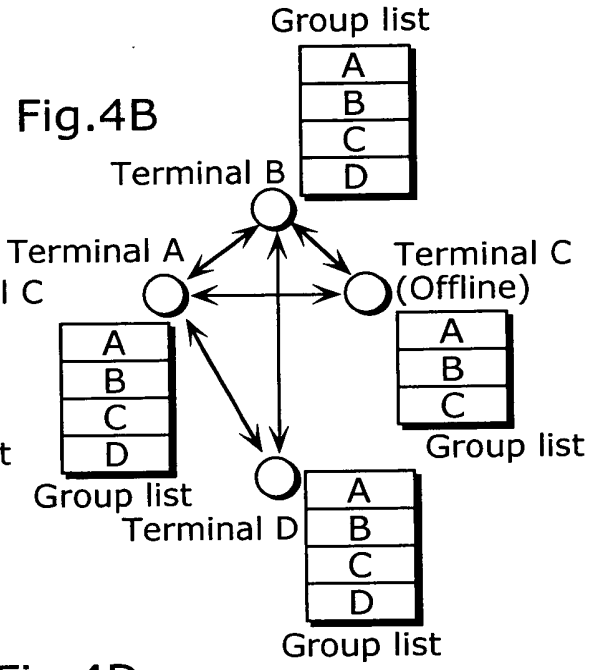


Fig.4C

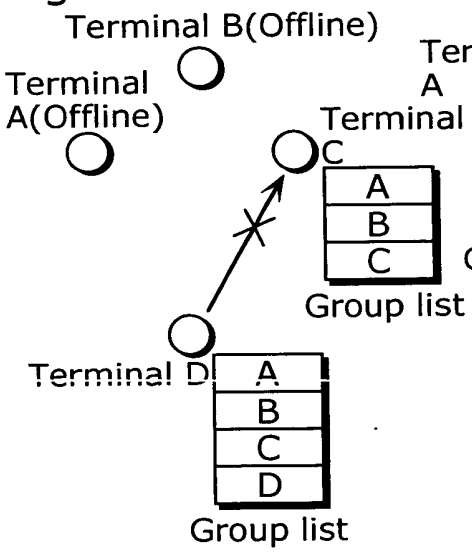


Fig.4D

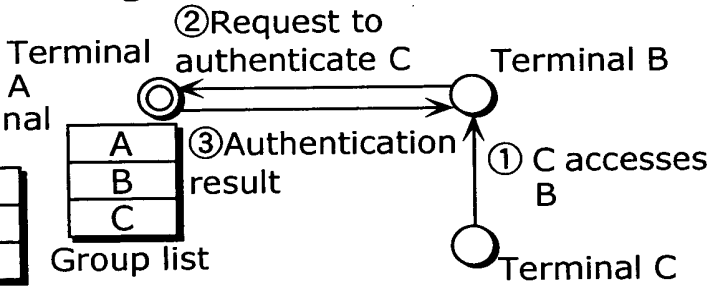


Fig.4E

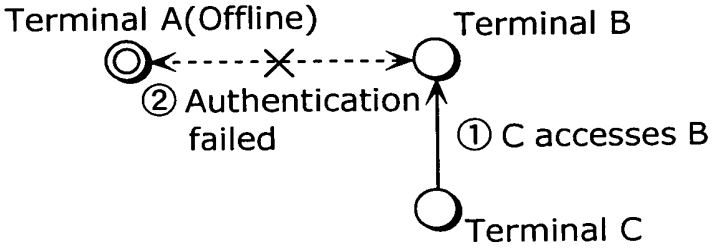


Fig.5A

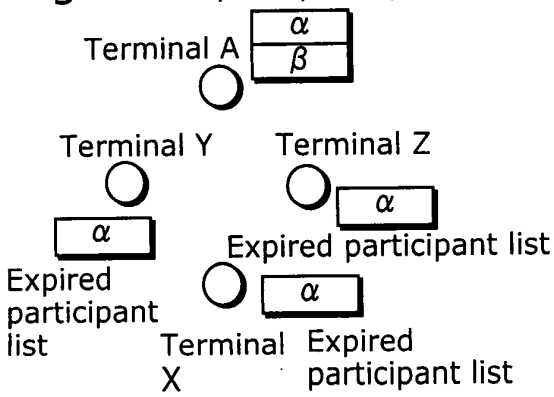


Fig.5B

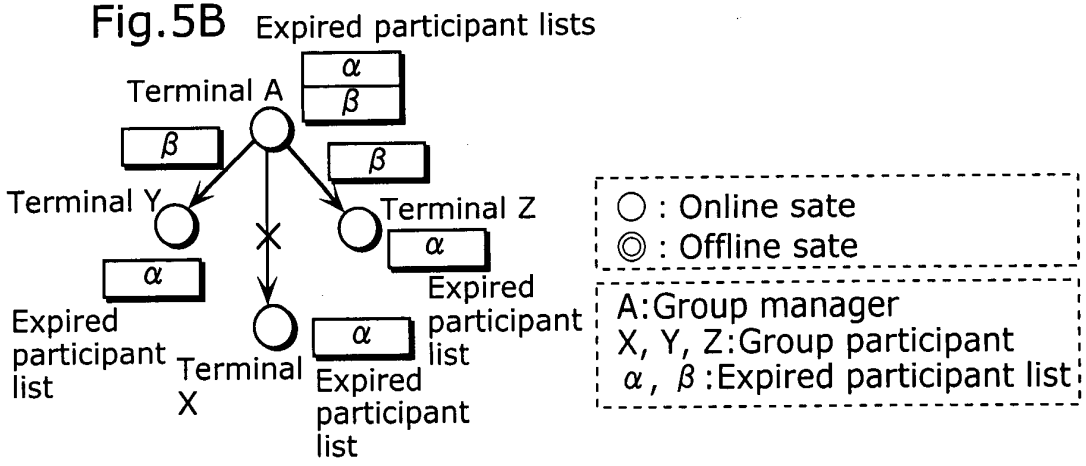


Fig.5C

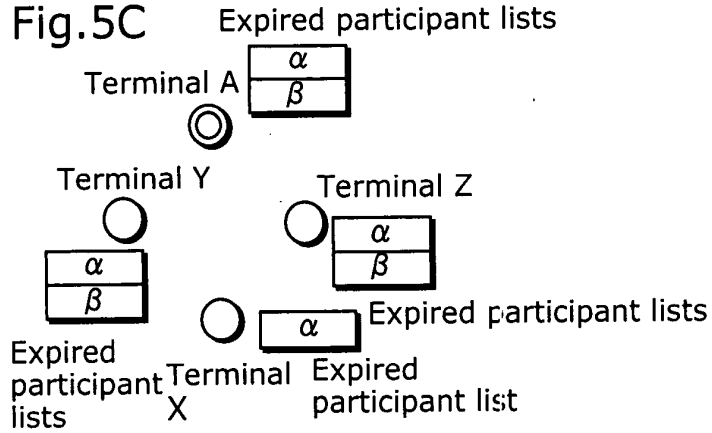
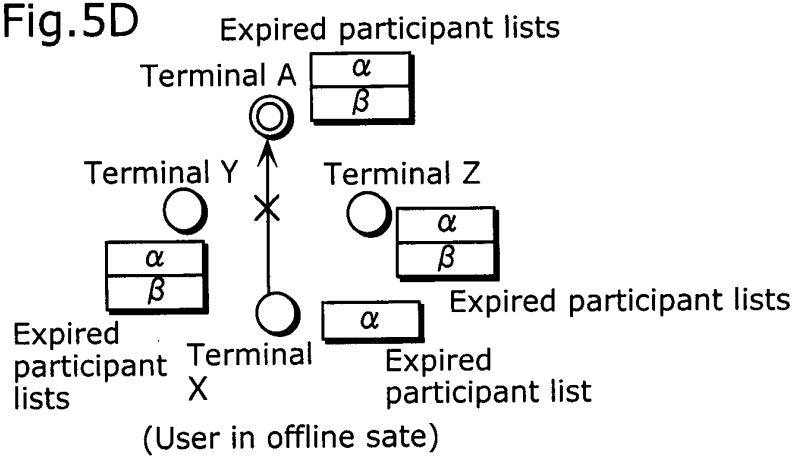


Fig.5D



(User in offline sate)

Fig.6

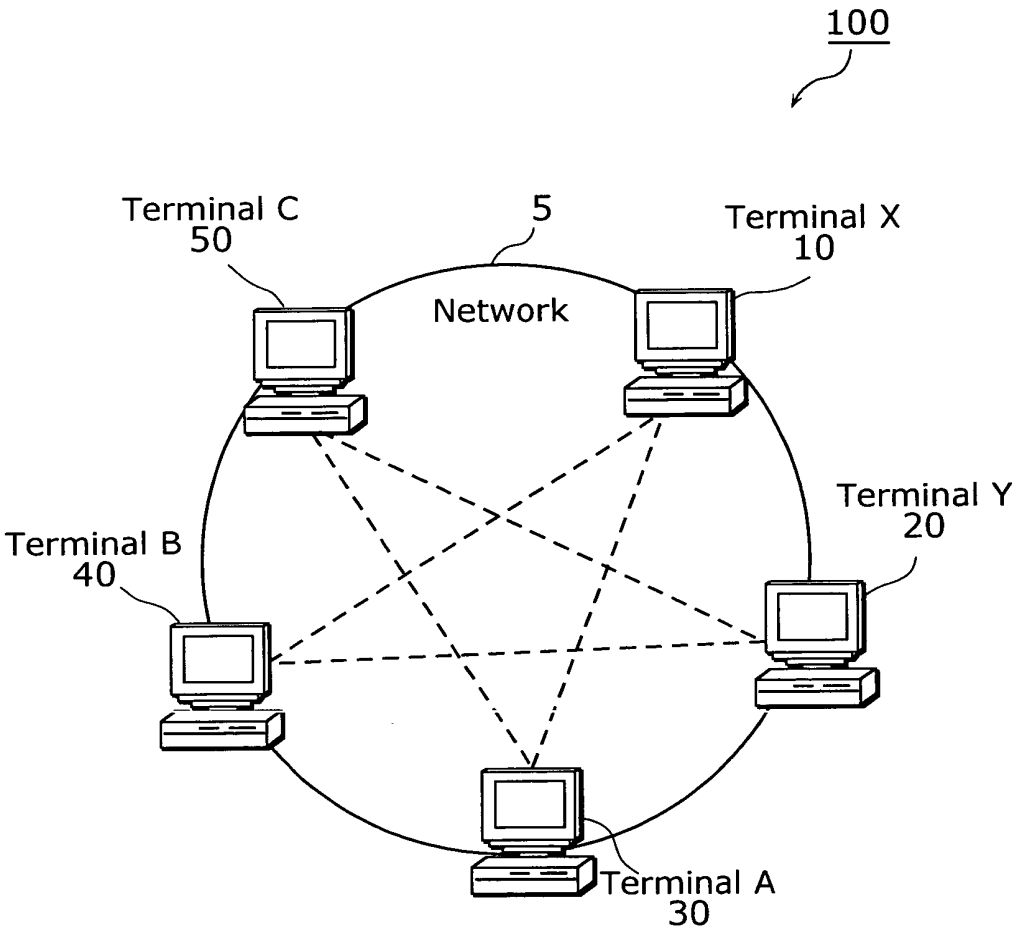

100
Terminal C
50
5
Terminal X
10
Network
Terminal Y
20
Terminal B
40
Terminal A
30

Fig.7

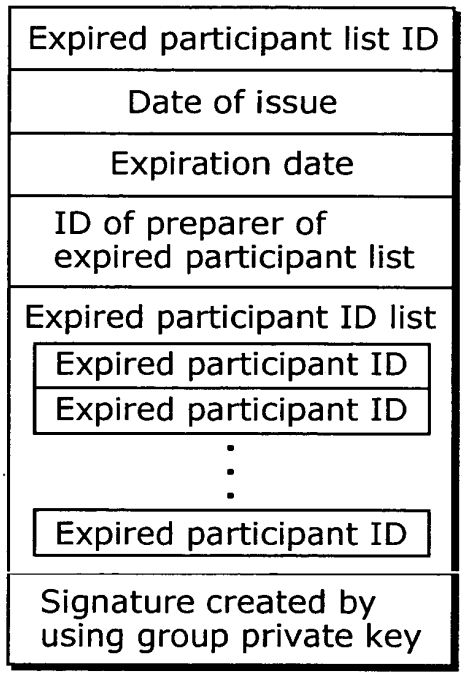

Expired participant list ID
Date of issue
Expiration date
ID of preparer of expired participant list
Expired participant ID list
Expired participant ID
Expired participant ID
Expired participant ID
Signature created by using group private key

Fig.8A

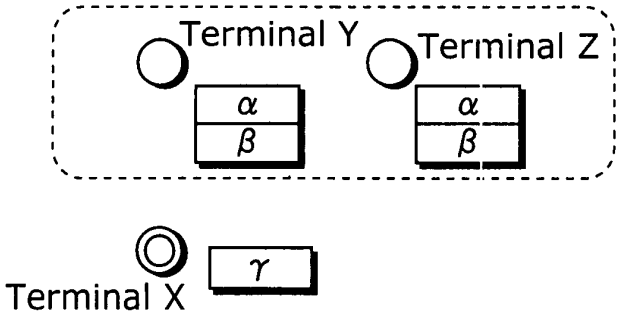


Fig.8B

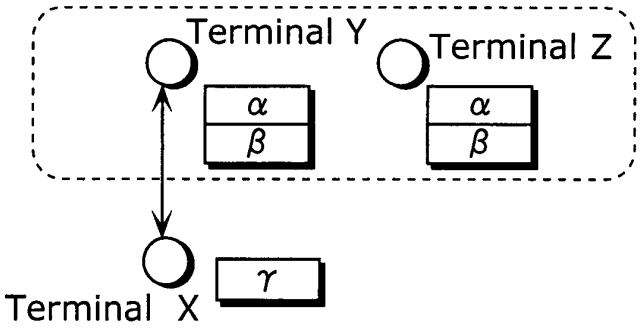


Fig.8C

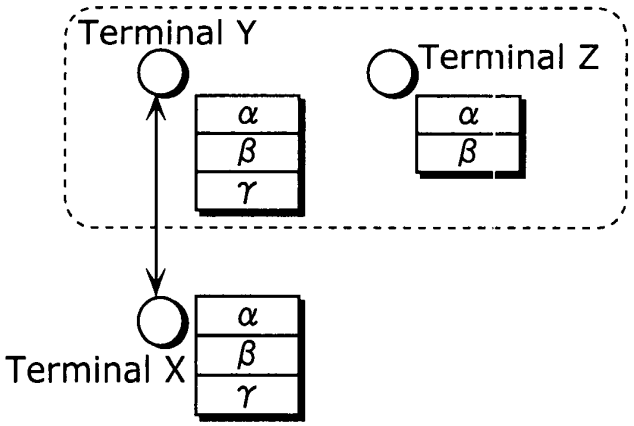


Fig.8D

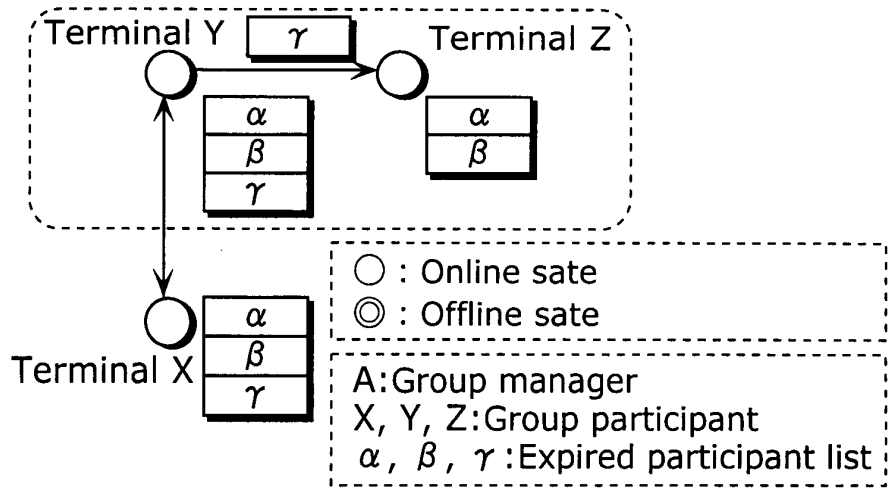


Fig.9

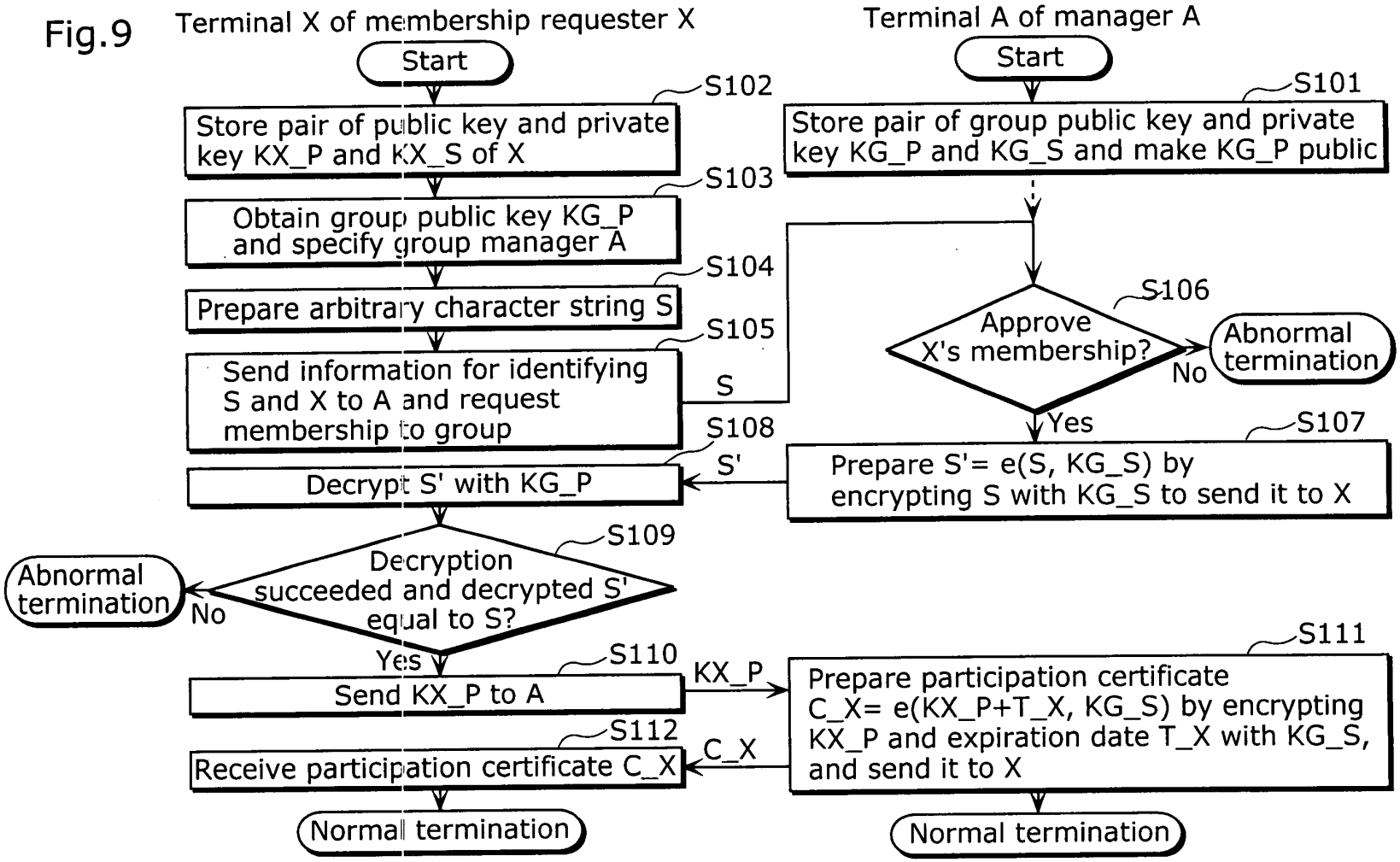

Terminal X of membership requester X
Terminal A of manager A
Start
Start
S102
Store pair of public key and private key KX_P and KX_S of X
S101
Store pair of group public key and private key KG_P and KG_S and make KG_P public
S103
Obtain group public key KG_P and specify group manager A
S104
Prepare arbitrary character string S
S105
Send information for identifying S and X to A and request membership to group
S
S106
Approve X's membership?
No
Abnormal termination
Yes
S107
Prepare S'= e(S, KG_S) by encrypting S with KG_S to send it to X
S'
S108
Decrypt S' with KG_P
S109
Decryption succeeded and decrypted S' equal to S?
No
Abnormal termination
Yes
S110
Send KX_P to A
KX_P
S111
Prepare participation certificate C_X= e(KX_P+T_X, KG_S) by encrypting KX_P and expiration date T_X with KG_S, and send it to X
C_X
S112
Receive participation certificate C_X
Normal termination
Normal termination

Fig.10

KX_P:Public key of X
KX_S:Private key of X
KG_P:Group public key
C_X=e(KX_P+T_X, KG_S):Group participation certificate of X

Fig.11

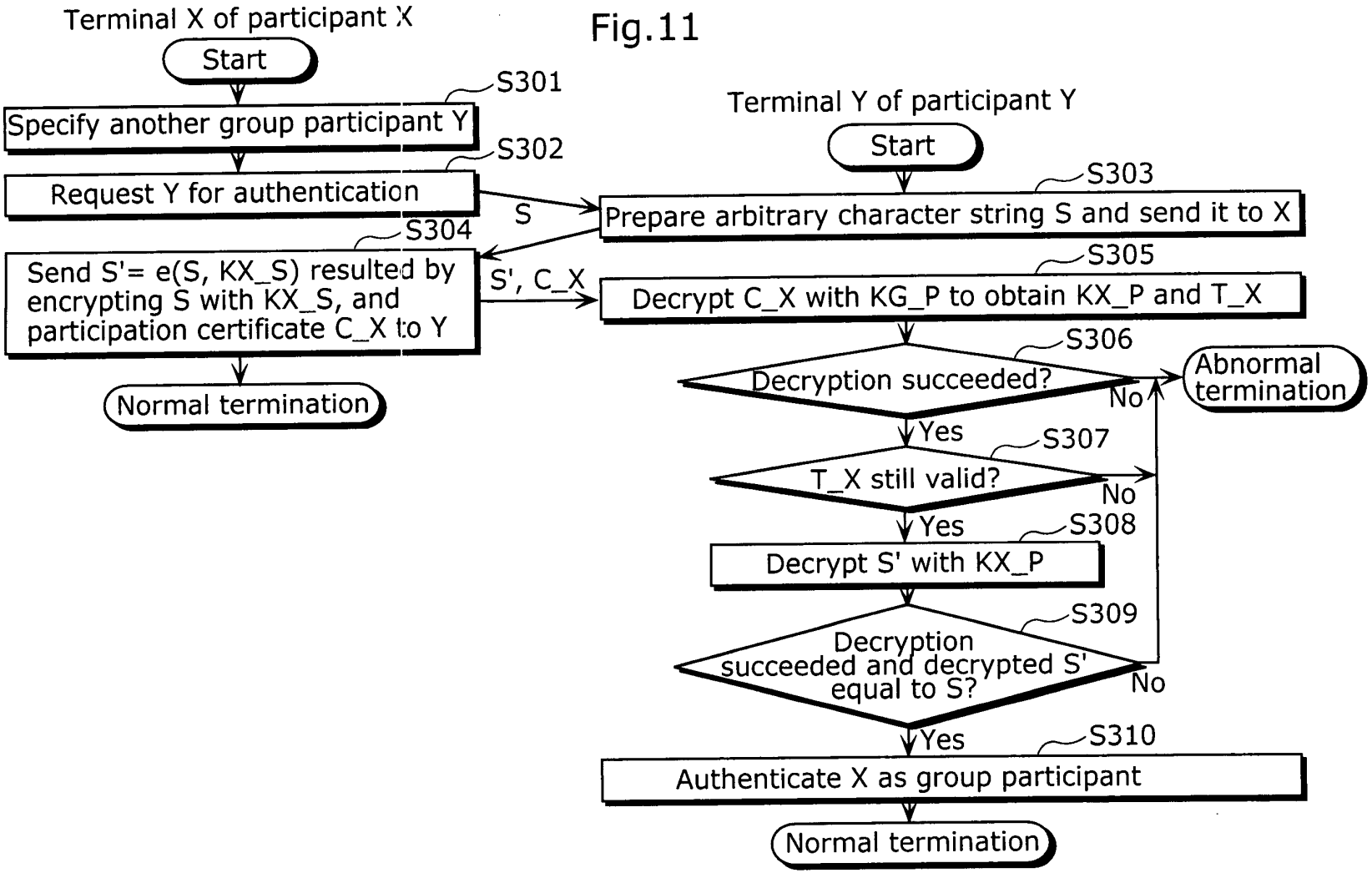

Terminal X of participant X
Start
S301
Specify another group participant Y
S302
Request Y for authentication
S
S304
Send S'= e(S, KX_S) resulted by encrypting S with KX_S, and participation certificate C_X to Y
S', C_X
Normal termination
Terminal Y of participant Y
Start
S303
Prepare arbitrary character string S and send it to X
S305
Decrypt C_X with KG_P to obtain KX_P and T_X
S306
Decryption succeeded?
No
Abnormal termination
Yes
S307
T_X still valid?
No
Yes
S308
Decrypt S' with KX_P
S309
Decryption succeeded and decrypted S' equal to S?
No
Yes
S310
Authenticate X as group participant
Normal termination

Fig.12

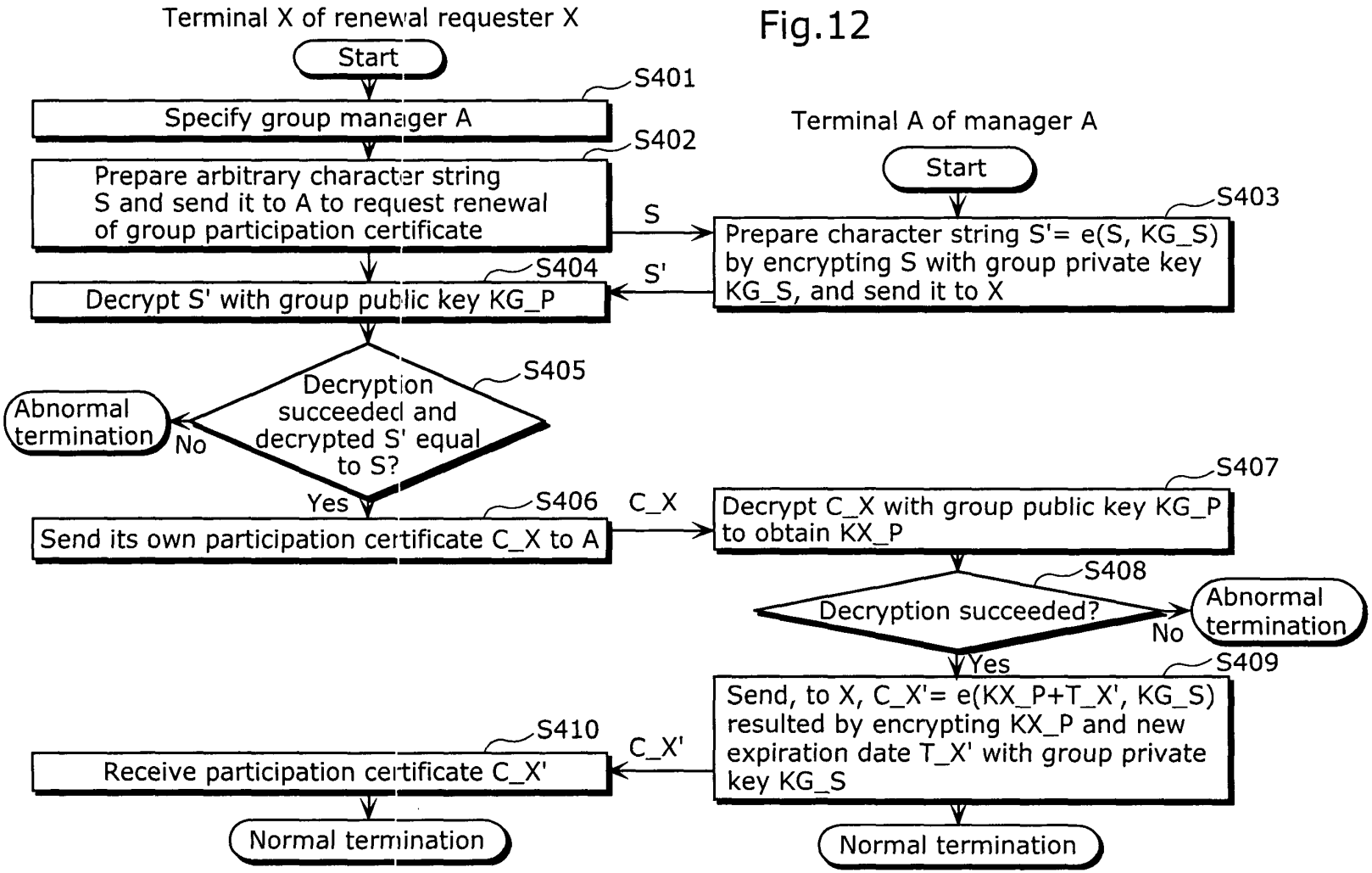

Terminal X of renewal requester X
Start
S401
Specify group manager A
S402
Prepare arbitrary character string S and send it to A to request renewal of group participation certificate
S
S404
Decrypt S' with group public key KG_P
S'
S405
Decryption succeeded and decrypted S' equal to S?
No
Abnormal termination
Yes
S406
Send its own participation certificate C_X to A
C_X
S410
Receive participation certificate C_X'
C_X'
Normal termination
Terminal A of manager A
Start
S403
Prepare character string S'= e(S, KG_S) by encrypting S with group private key KG_S, and send it to X
S407
Decrypt C_X with group public key KG_P to obtain KX_P
S408
Decryption succeeded?
No
Abnormal termination
Yes
S409
Send, to X, C_X'= e(KX_P+T_X', KG_S) resulted by encrypting KX_P and new expiration date T_X' with group private key KG_S
Normal termination

Fig.13

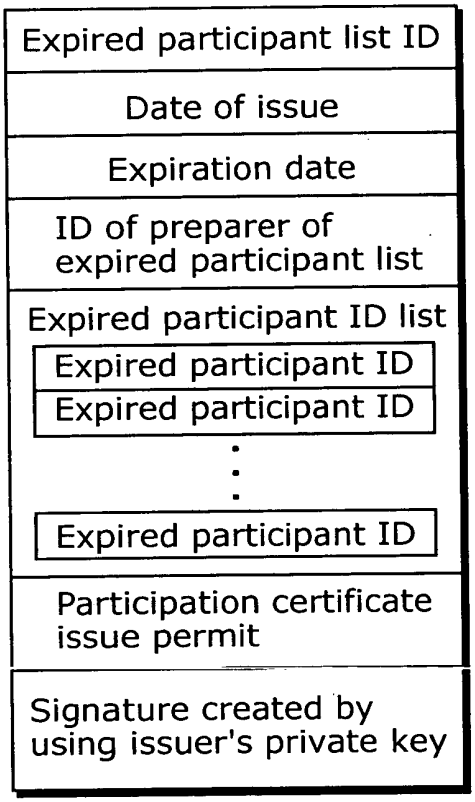

Expired participant list ID
Date of issue
Expiration date
ID of preparer of expired participant list
Expired participant ID list
Expired participant ID
Expired participant ID
Expired participant ID
Participation certificate issue permit
Signature created by using issuer's private key

Fig.14

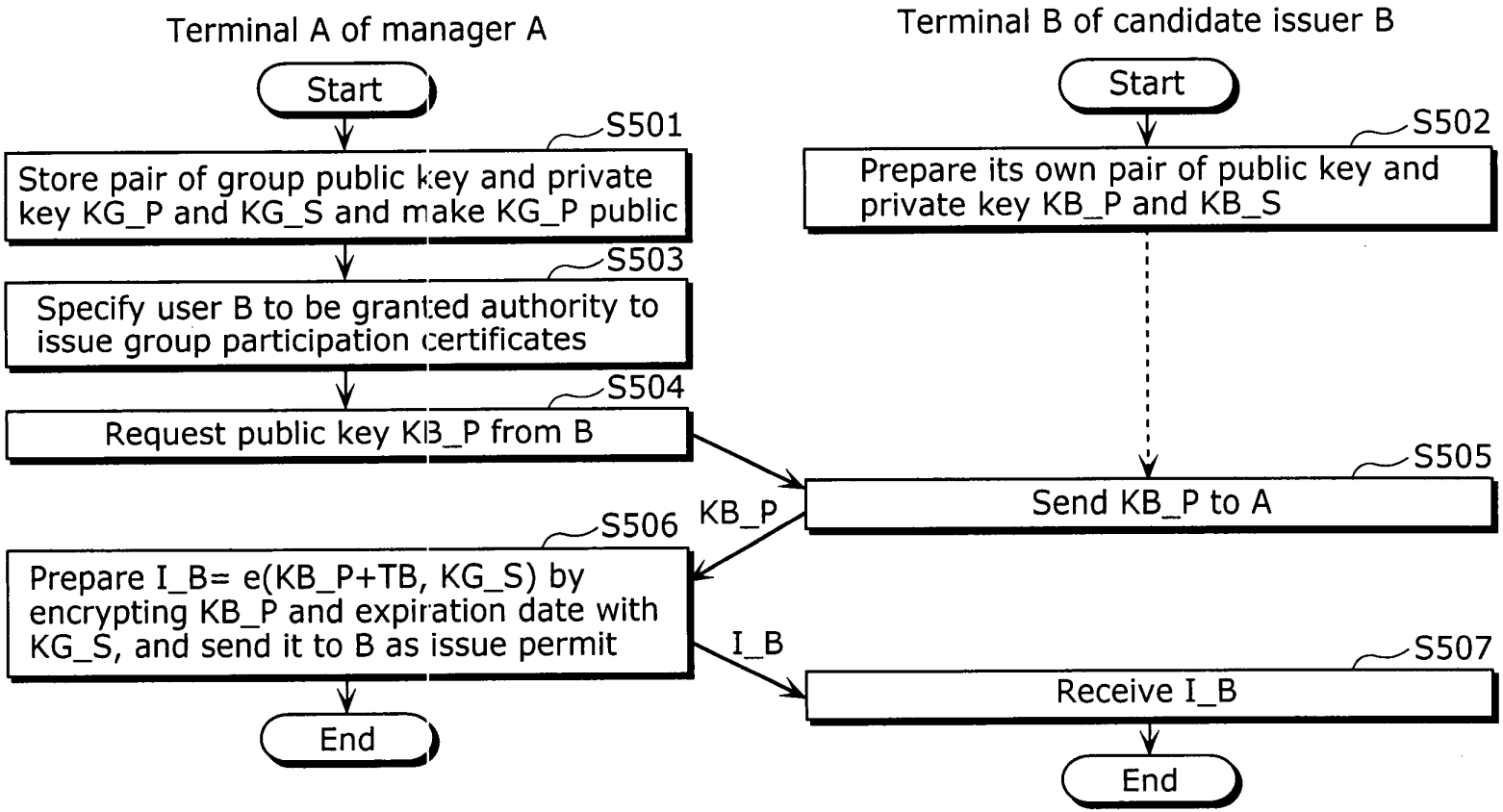

Terminal A of manager A
Start
S501
Store pair of group public key and private key KG_P and KG_S and make KG_P public
S503
Specify user B to be granted authority to issue group participation certificates
S504
Request public key KB_P from B
S506
Prepare I_B= e(KB_P+TB, KG_S) by encrypting KB_P and expiration date with KG_S, and send it to B as issue permit
End
KB_P
I_B
Terminal B of candidate issuer B
Start
S502
Prepare its own pair of public key and private key KB_P and KB_S
S505
Send KB_P to A
S507
Receive I_B
End

Fig.15

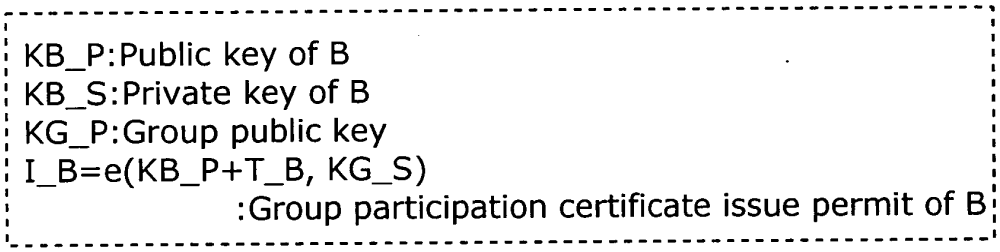

KB_P:Public key of B
KB_S:Private key of B
KG_P:Group public key
I_B=e(KB_P+T_B, KG_S)
:Group participation certificate issue permit of B

Fig.16

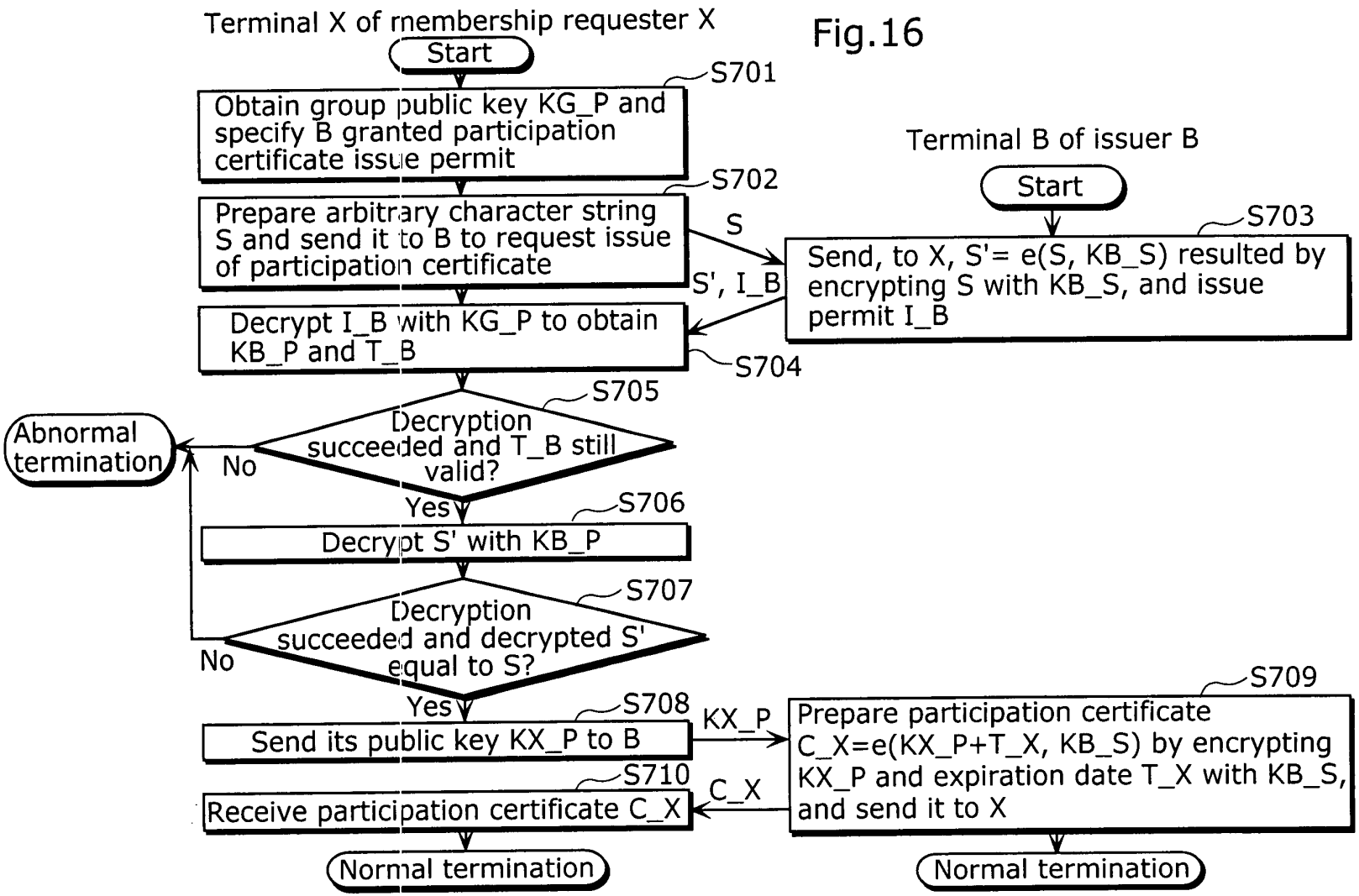

Terminal X of membership requester X
Start
S701
Obtain group public key KG_P and specify B granted participation certificate issue permit
S702
Prepare arbitrary character string S and send it to B to request issue of participation certificate
S
S', I_B
Decrypt I_B with KG_P to obtain KB_P and T_B
S704
S705
Decryption succeeded and T_B still valid?
No
Abnormal termination
Yes
S706
Decrypt S' with KB_P
S707
Decryption succeeded and decrypted S' equal to S?
No
Yes
S708
Send its public key KX_P to B
KX_P
S710
C_X
Receive participation certificate C_X
Normal termination
Terminal B of issuer B
Start
S703
Send, to X, S'= e(S, KB_S) resulted by encrypting S with KB_S, and issue permit I_B
S709
Prepare participation certificate C_X=e(KX_P+T_X, KB_S) by encrypting KX_P and expiration date T_X with KB_S, and send it to X
Normal termination

Fig.17

KX_P:Public key of X
KX_S:Private key of X
KG_P:Group public key
I_B=e(KB_P+T_B, KG_S)
:Group participation certificate issue permit of B
C_X=e(KX_P+T_X, KB_S):Group participation certificate of X

Fig.18

KY_P:Public key of Y
KY_S:Private key of Y
KG_P:Group public key
I_C=e(KC_P+T_C, KG_S)
:Group participation certificate issue permit of another issuer C
C_Y=e(KX_P+T_X, KB_S)
:Group participation certificate of Y issued by C

Fig.19

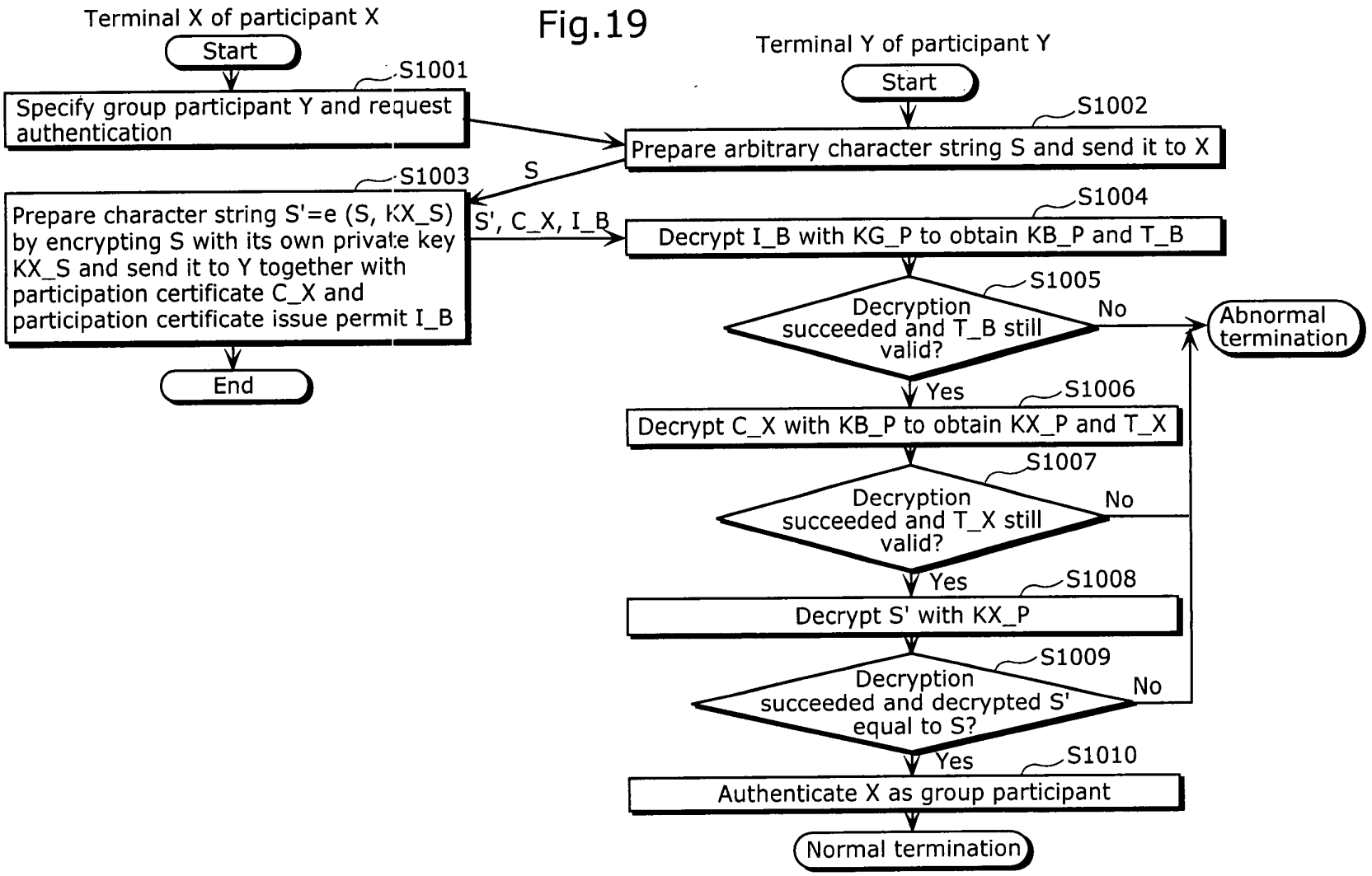

Terminal X of participant X
Start
S1001
Specify group participant Y and request authentication
S1003
Prepare character string S'=e (S, KX_S) by encrypting S with its own private key KX_S and send it to Y together with participation certificate C_X and participation certificate issue permit I_B
End
S
S', C_X, I_B
Terminal Y of participant Y
Start
S1002
Prepare arbitrary character string S and send it to X
S1004
Decrypt I_B with KG_P to obtain KB_P and T_B
S1005
Decryption succeeded and T_B still valid?
No
Abnormal termination
Yes
S1006
Decrypt C_X with KB_P to obtain KX_P and T_X
S1007
Decryption succeeded and T_X still valid?
No
Yes
S1008
Decrypt S' with KX_P
S1009
Decryption succeeded and decrypted S' equal to S?
No
Yes
S1010
Authenticate X as group participant
Normal termination

Fig.20

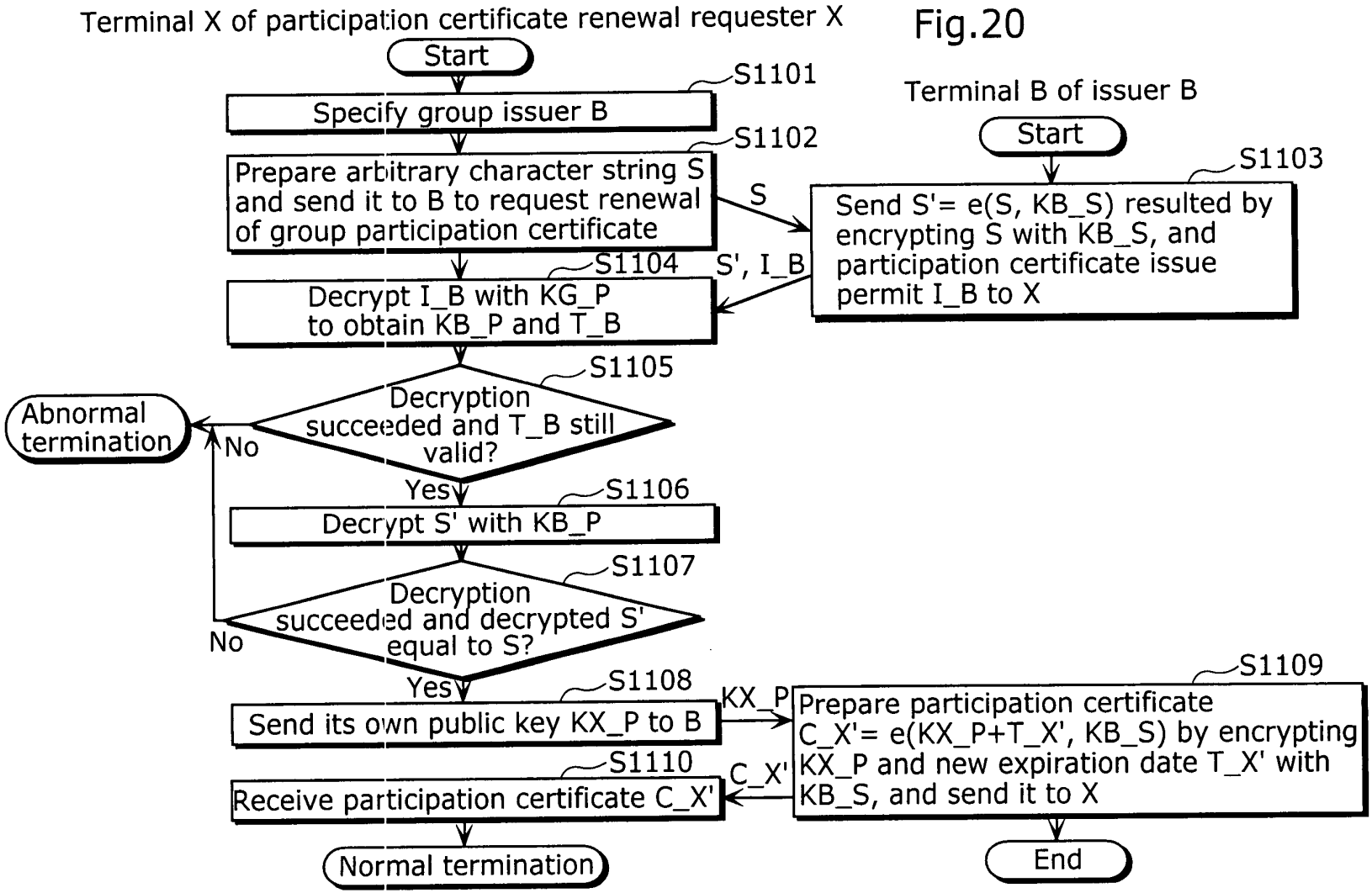

Terminal X of participation certificate renewal requester X
Start
S1101
Specify group issuer B
S1102
Prepare arbitrary character string S and send it to B to request renewal of group participation certificate
S
S1104
S', I_B
Decrypt I_B with KG_P to obtain KB_P and T_B
S1105
Decryption succeeded and T_B still valid?
No
Abnormal termination
Yes
S1106
Decrypt S' with KB_P
S1107
Decryption succeeded and decrypted S' equal to S?
No
Yes
S1108
KX_P
Send its own public key KX_P to B
S1110
C_X'
Receive participation certificate C_X'
Normal termination
Terminal B of issuer B
Start
S1103
Send S'= e(S, KB_S) resulted by encrypting S with KB_S, and participation certificate issue permit I_B to X
S1109
Prepare participation certificate C_X'= e(KX_P+T_X', KB_S) by encrypting KX_P and new expiration date T_X' with KB_S, and send it to X
End

Fig.21

KX_P:Public key of X
KX_S:Private key of X
KG_P:Group public key
I_B=e(KB_P+T_B, KG_S)
:Group participation certificate issue permit of B
C_X=e(KX_P+T_X', KB_S):Group participation certificate of X

Fig.22

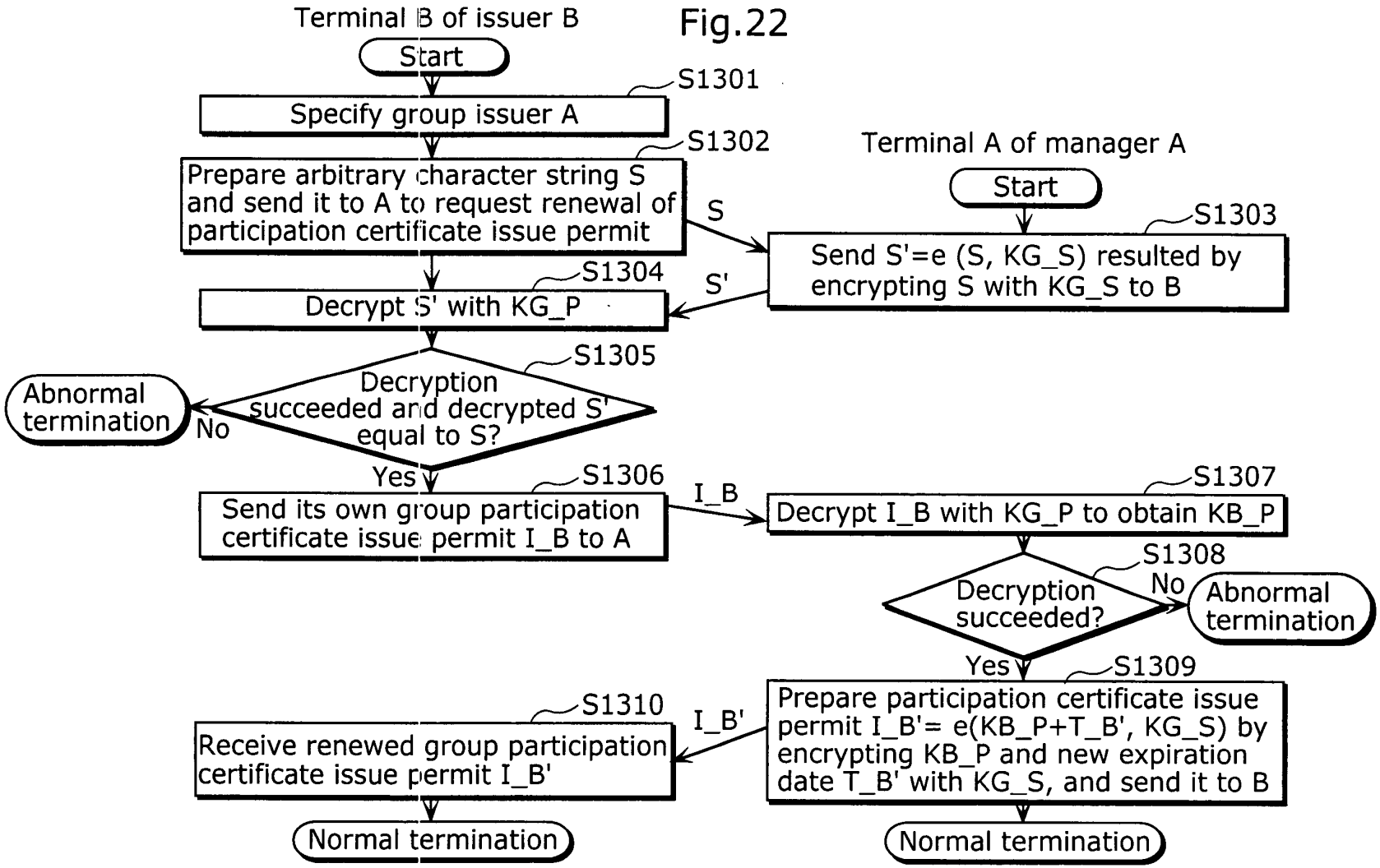

Terminal B of issuer B
Start
S1301
Specify group issuer A
S1302
Prepare arbitrary character string S and send it to A to request renewal of participation certificate issue permit
S
Terminal A of manager A
Start
S1303
Send S'=e (S, KG_S) resulted by encrypting S with KG_S to B
S'
S1304
Decrypt S' with KG_P
S1305
Decryption succeeded and decrypted S' equal to S?
No
Abnormal termination
Yes
S1306
Send its own group participation certificate issue permit I_B to A
I_B
S1307
Decrypt I_B with KG_P to obtain KB_P
S1308
Decryption succeeded?
No
Abnormal termination
Yes
S1309
Prepare participation certificate issue permit I_B'= e(KB_P+T_B', KG_S) by encrypting KB_P and new expiration date T_B' with KG_S, and send it to B
I_B'
S1310
Receive renewed group participation certificate issue permit I_B'
Normal termination
Normal termination

Fig.23

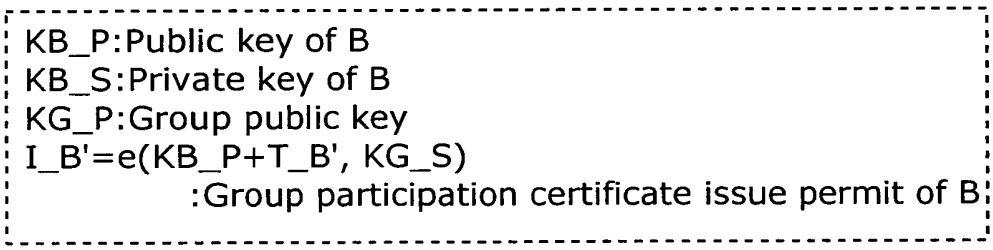

KB_P:Public key of B
KB_S:Private key of B
KG_P:Group public key
I_B'=e(KB_P+T_B', KG_S)
:Group participation certificate issue permit of B

Fig.24

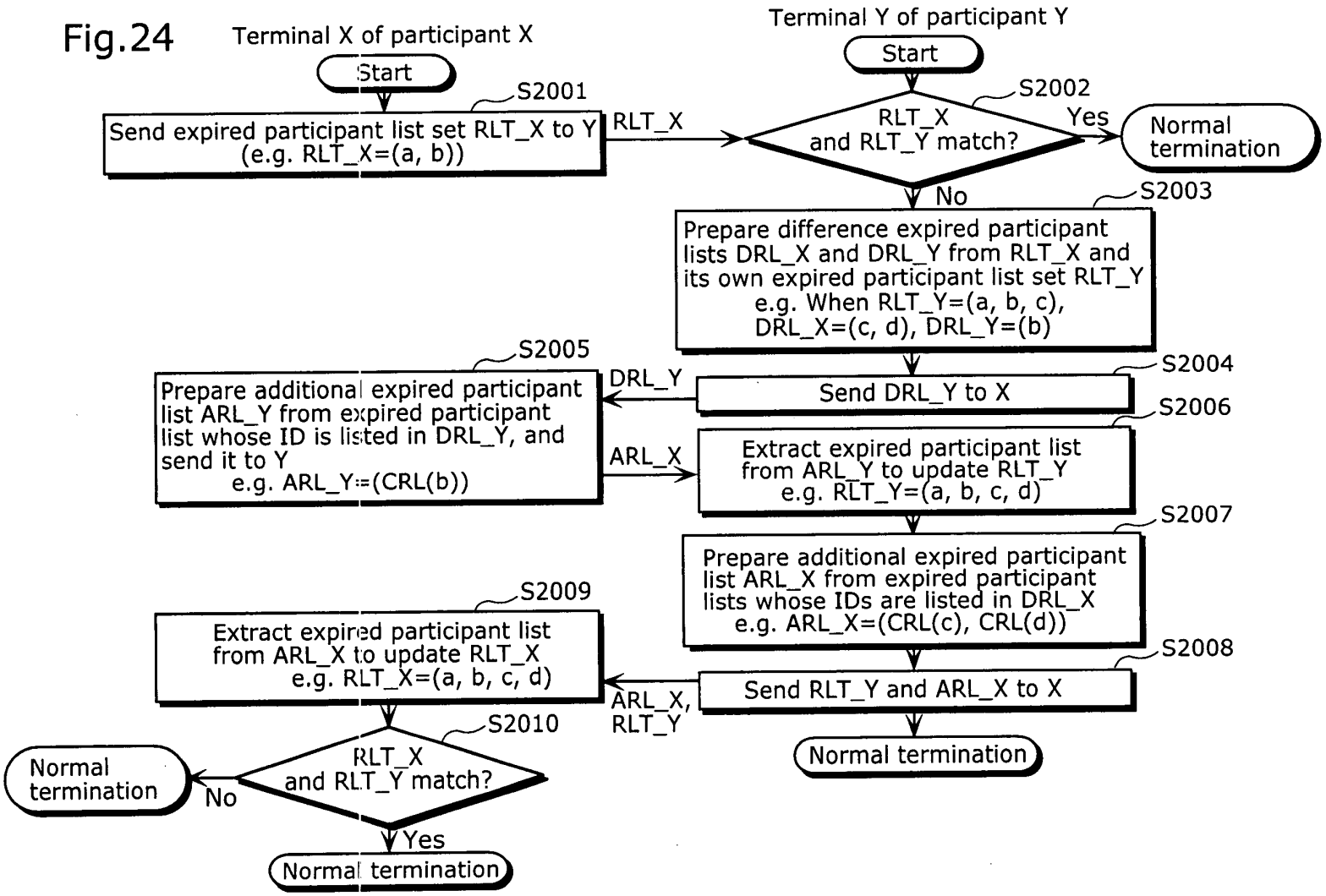

Terminal X of participant X
Start
S2001
Send expired participant list set RLT_X to Y
(e.g. RLT_X=(a, b))
RLT_X
Terminal Y of participant Y
Start
S2002
RLT_X
and RLT_Y match?
Yes
Normal termination
No
S2003
Prepare difference expired participant lists DRL_X and DRL_Y from RLT_X and its own expired participant list set RLT_Y
e.g. When RLT_Y=(a, b, c), DRL_X=(c, d), DRL_Y=(b)
S2004
Send DRL_Y to X
DRL_Y
S2005
Prepare additional expired participant list ARL_Y from expired participant list whose ID is listed in DRL_Y, and send it to Y
e.g. ARL_Y=(CRL(b))
ARL_X
S2006
Extract expired participant list from ARL_Y to update RLT_Y
e.g. RLT_Y=(a, b, c, d)
S2007
Prepare additional expired participant list ARL_X from expired participant lists whose IDs are listed in DRL_X
e.g. ARL_X=(CRL(c), CRL(d))
S2008
Send RLT_Y and ARL_X to X
ARL_X, RLT_Y
Normal termination
S2009
Extract expired participant list from ARL_X to update RLT_X
e.g. RLT_X=(a, b, c, d)
S2010
RLT_X
and RLT_Y match?
Normal termination
No
Yes
Normal termination

Fig.25

RLT_X:Collection of expired participant lists (expired participant list set) possessed by X
DRL_X:Collection of expired participant lists (difference expired participant list) not possessed by X
ARL_X:Collection of expired participant lists (additional expired participant list) not possessed by X
a, b,c, d, ···:Expired participant list ID
CRL(a):Expired participant list whose ID is "a"

Fig.26

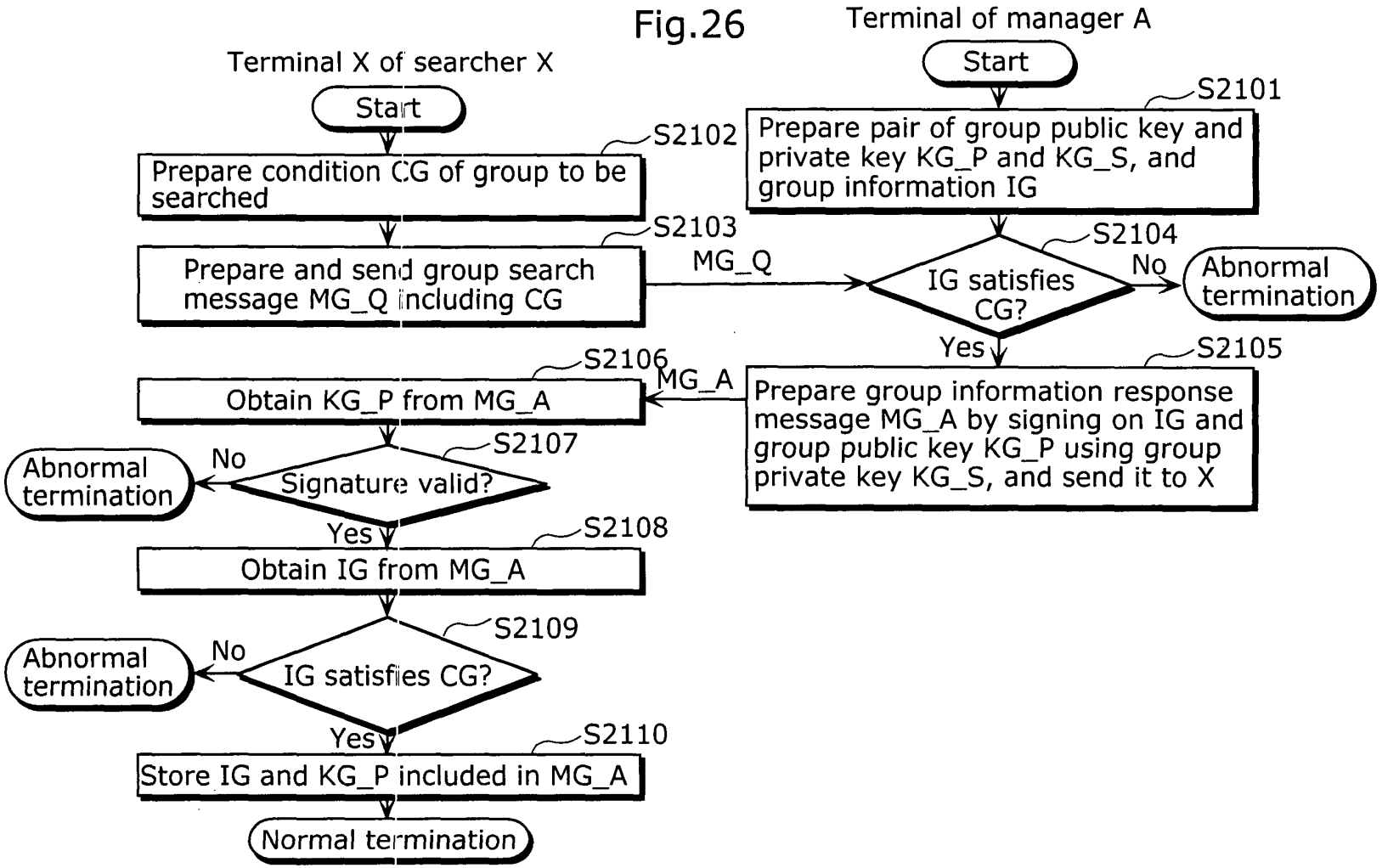

Terminal X of searcher X
Start
S2102
Prepare condition CG of group to be searched
S2103
Prepare and send group search message MG_Q including CG
MG_Q
Terminal of manager A
Start
S2101
Prepare pair of group public key and private key KG_P and KG_S, and group information IG
S2104
IG satisfies CG?
No
Abnormal termination
Yes
S2105
Prepare group information response message MG_A by signing on IG and group public key KG_P using group private key KG_S, and send it to X
MG_A
S2106
Obtain KG_P from MG_A
S2107
Signature valid?
No
Abnormal termination
Yes
S2108
Obtain IG from MG_A
S2109
IG satisfies CG?
No
Abnormal termination
Yes
S2110
Store IG and KG_P included in MG_A
Normal termination

Fig.27


KG_P:Group public key
IG:Information about group
(Category, information required for participation etc.)

Fig.28

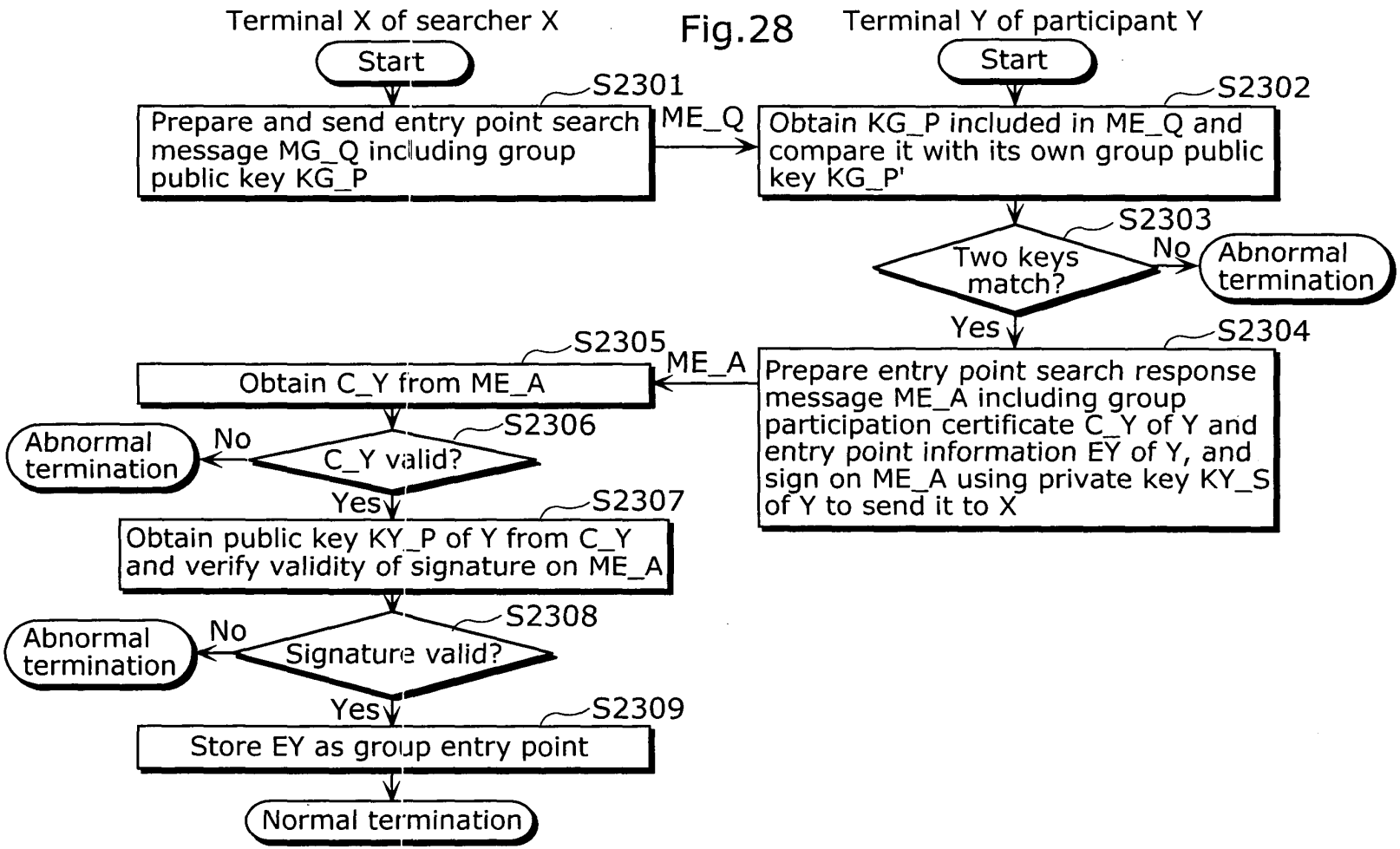

Terminal X of searcher X
Start
S2301
Prepare and send entry point search message MG_Q including group public key KG_P
ME_Q
Terminal Y of participant Y
Start
S2302
Obtain KG_P included in ME_Q and compare it with its own group public key KG_P'
S2303
Two keys match?
No
Abnormal termination
Yes
S2304
Prepare entry point search response message ME_A including group participation certificate C_Y of Y and entry point information EY of Y, and sign on ME_A using private key KY_S of Y to send it to X
ME_A
S2305
Obtain C_Y from ME_A
S2306
C_Y valid?
No
Abnormal termination
Yes
S2307
Obtain public key KY_P of Y from C_Y and verify validity of signature on ME_A
S2308
Signature valid?
No
Abnormal termination
Yes
S2309
Store EY as group entry point
Normal termination

Fig.29

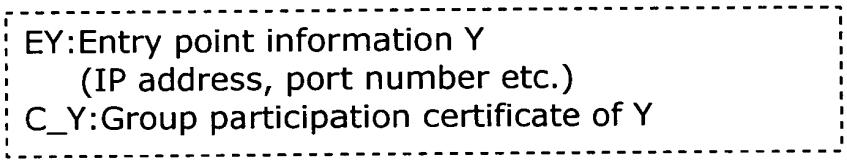

EY:Entry point information Y
(IP address, port number etc.)
C_Y:Group participation certificate of Y

Fig.30

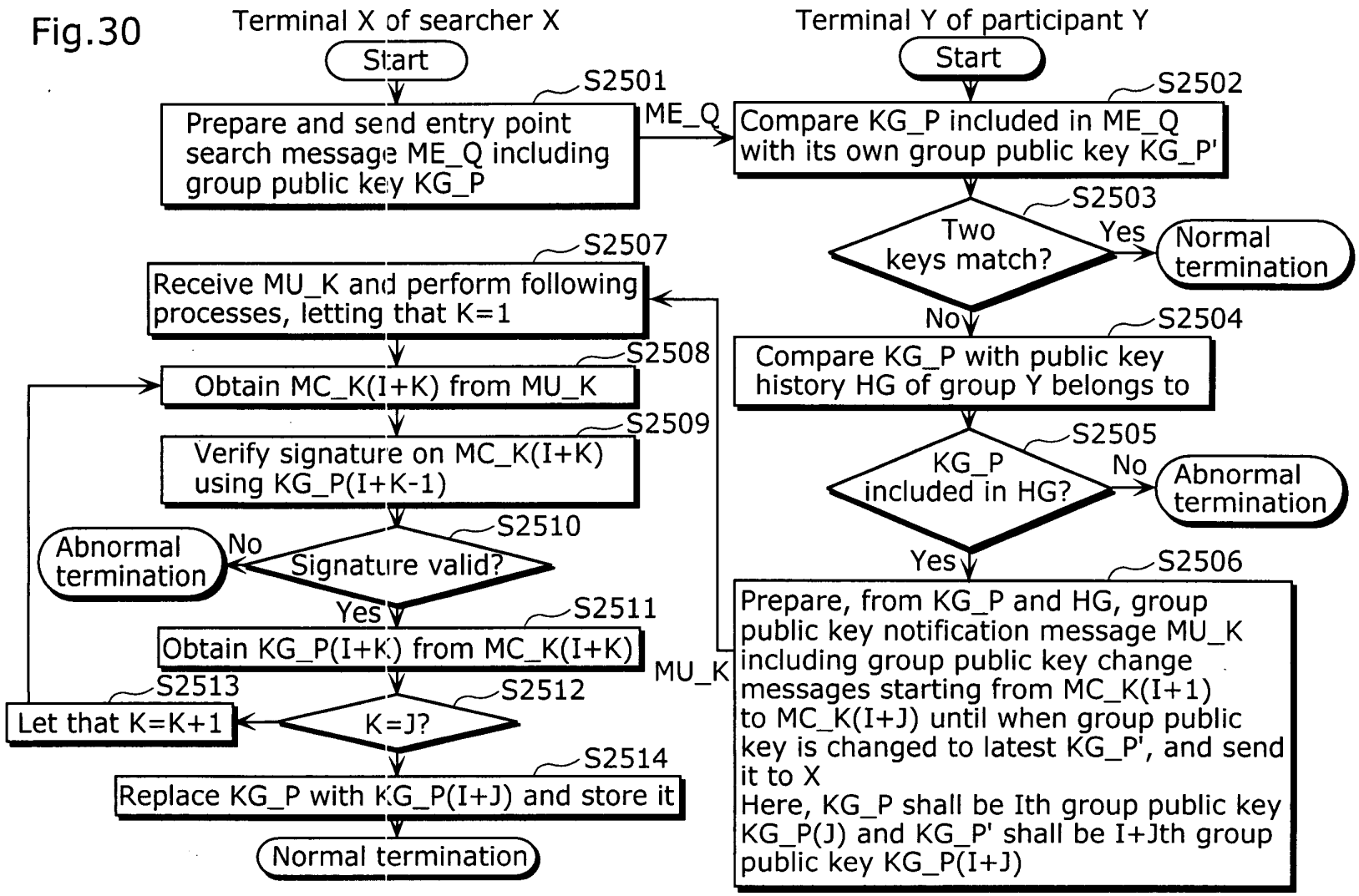

Terminal X of searcher X
Terminal Y of participant Y
Start
S2501
Prepare and send entry point search message ME_Q including group public key KG_P
ME_Q
Start
S2502
Compare KG_P included in ME_Q with its own group public key KG_P'
S2503
Two keys match?
Yes
Normal termination
No
S2504
Compare KG_P with public key history HG of group Y belongs to
S2505
KG_P included in HG?
No
Abnormal termination
Yes
S2506
Prepare, from KG_P and HG, group public key notification message MU_K including group public key change messages starting from MC_K(I+1) to MC_K(I+J) until when group public key is changed to latest KG_P', and send it to X
Here, KG_P shall be Ith group public key KG_P(J) and KG_P' shall be I+Jth group public key KG_P(I+J)
MU_K
S2507
Receive MU_K and perform following processes, letting that K=1
S2508
Obtain MC_K(I+K) from MU_K
S2509
Verify signature on MC_K(I+K) using KG_P(I+K-1)
S2510
Signature valid?
No
Abnormal termination
Yes
S2511
Obtain KG_P(I+K) from MC_K(I+K)
S2512
K=J?
S2513
Let that K=K+1
S2514
Replace KG_P with KG_P(I+J) and store it
Normal termination

Fig.31

KG_P':Latest group public key

Fig.32

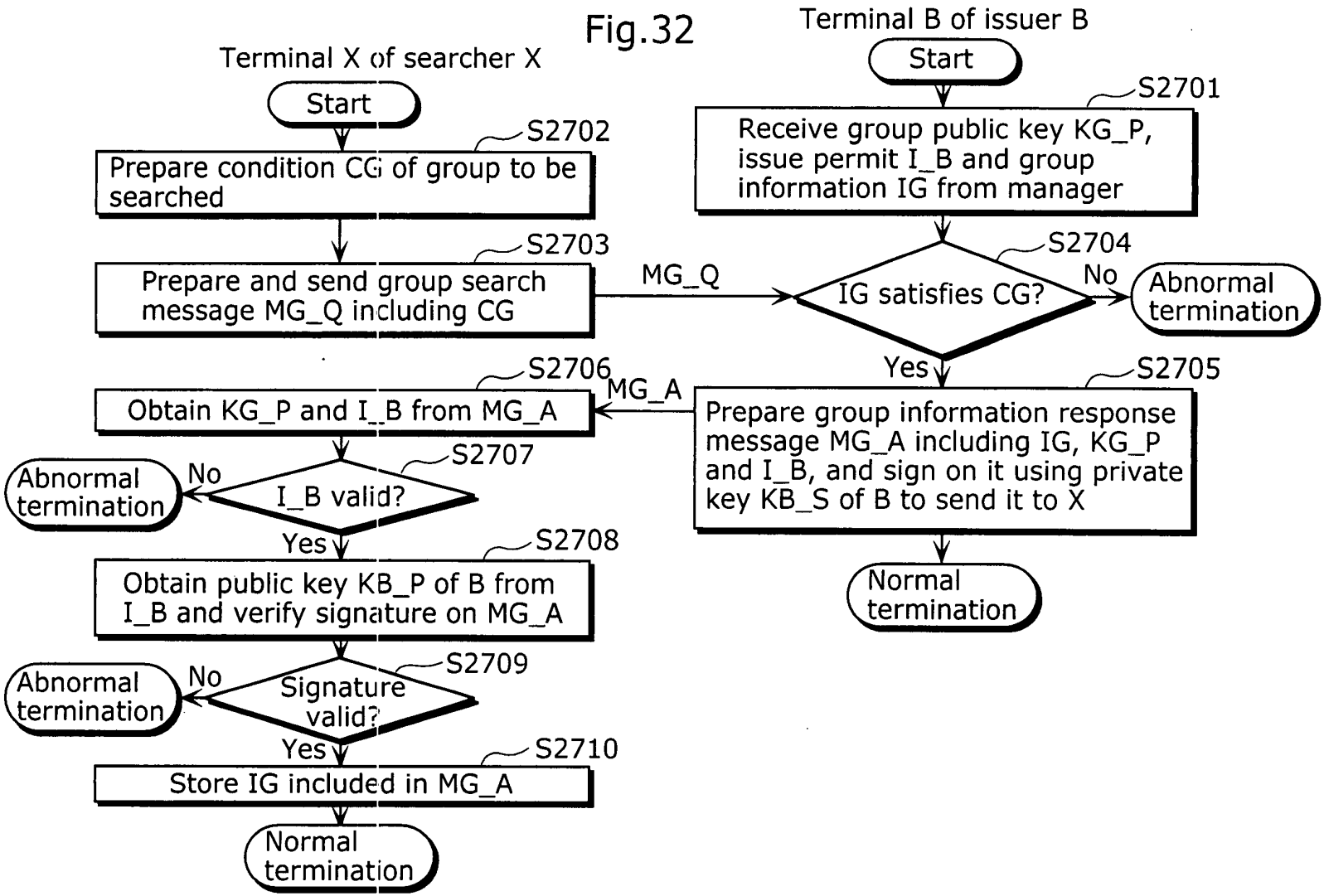

Terminal X of searcher X
Start
S2702
Prepare condition CG of group to be searched
S2703
Prepare and send group search message MG_Q including CG
MG_Q
Terminal B of issuer B
Start
S2701
Receive group public key KG_P, issue permit I_B and group information IG from manager
S2704
IG satisfies CG?
No
Abnormal termination
Yes
S2705
Prepare group information response message MG_A including IG, KG_P and I_B, and sign on it using private key KB_S of B to send it to X
MG_A
Normal termination
S2706
Obtain KG_P and I_B from MG_A
S2707
I_B valid?
No
Abnormal termination
Yes
S2708
Obtain public key KB_P of B from I_B and verify signature on MG_A
S2709
Signature valid?
No
Abnormal termination
Yes
S2710
Store IG included in MG_A
Normal termination

Fig.33

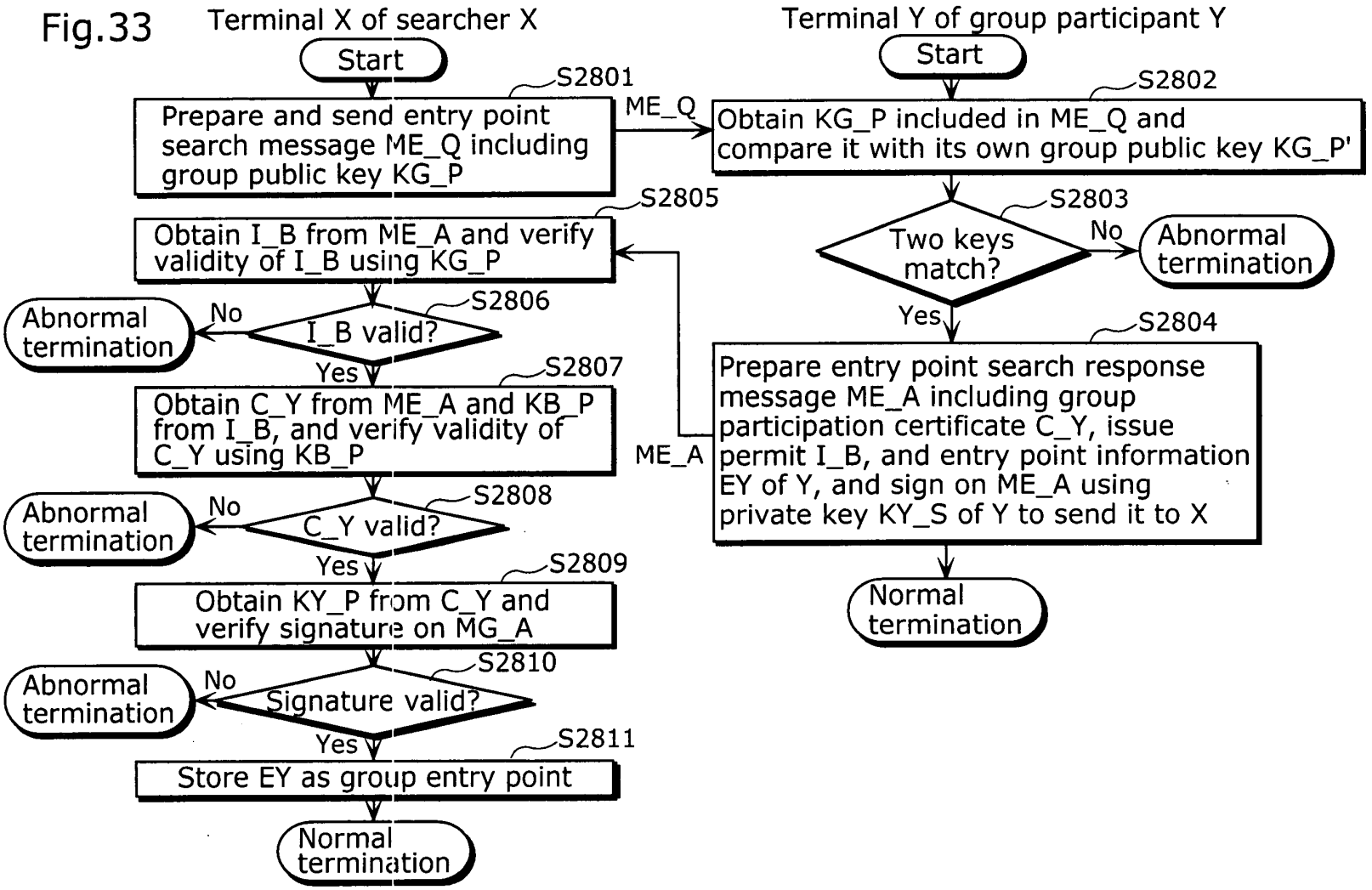
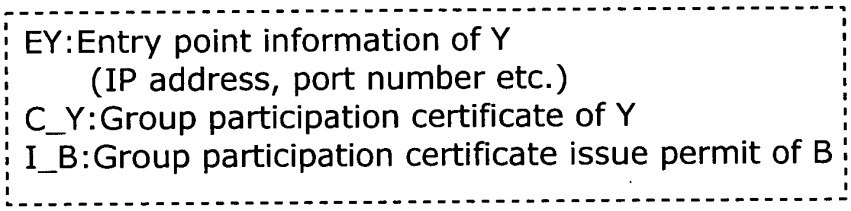

Terminal X of searcher X
Terminal Y of group participant Y
Start
S2801
Prepare and send entry point search message ME_Q including group public key KG_P
ME_Q
Start
S2802
Obtain KG_P included in ME_Q and compare it with its own group public key KG_P'
S2803
Two keys match?
No
Abnormal termination
Yes
S2804
Prepare entry point search response message ME_A including group participation certificate C_Y, issue permit I_B, and entry point information EY of Y, and sign on ME_A using private key KY_S of Y to send it to X
ME_A
Normal termination
S2805
Obtain I_B from ME_A and verify validity of I_B using KG_P
S2806
I_B valid?
No
Abnormal termination
Yes
S2807
Obtain C_Y from ME_A and KB_P from I_B, and verify validity of C_Y using KB_P
S2808
C_Y valid?
No
Abnormal termination
Yes
S2809
Obtain KY_P from C_Y and verify signature on MG_A
S2810
Signature valid?
No
Abnormal termination
Yes
S2811
Store EY as group entry point
Normal termination

Fig.34


EY:Entry point information of Y
(IP address, port number etc.)
C_Y:Group participation certificate of Y
I_B:Group participation certificate issue permit of B